AMBIENT-IT

+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated 05/28/2024

Sign up

Pentest Web training: OWASP API

3 days (21 hours)

PRESENTATION

This Pentest Web training course focuses on the most frequent and most critical web vulnerabilities (chosen from the OWASP top 10). After a brief theoretical presentation, a lab will be set up with an application that you will have to compromise.

Starting with no access at all, your goal will be to bypass authentication and then execute remote system code on the server (RCE).

To make the practical work more fun, it is organized in the form of a CTF, where participants compete either as a team or individually (your choice).

After the exploitation phase, you will be offered the opportunity to correct the vulnerability and verify by practical means (penetration testing) that it can no longer be exploited. In addition to training in offensive security, you will also learn how to correct vulnerabilities in your network.

Depending on the level of participants and the length of the course (from 1 to 3 days), the program can be broken down into several levels: from the discovery of web pentesting to advanced exploitation techniques.

Depending on progress, the following topics in particular may be covered: brute force attacks and fuzzing, partitioning and access control, exploiting blind SQL injections, Cross-Site Scripting (XSS) and WAF/CSP bypassing, Cross-Site Origin Resource Sharing (CORS), XML External Entity (XXE), file upload form.

OBJECTIVES

- Learn about the most frequent and critical security vulnerabilities
- Master penetration testing methodology to protect your infrastructure
- Efficiently correct vulnerabilities

TARGET AUDIENCE

- Developers
- Project managers
- SSI technicians
- Auditors
- Sliders
- CISO
- Ethical hackers
- Network architects

Prerequisites

- Basic knowledge of web security
- Knowledge of a programming language

Technical requirements

- A good Internet connection is required to connect to the labs
- Burp Suite installed
- Download VM Kali and Mobexeler

OUR WEB PENETRATION TEST TRAINING PROGRAM

Presentation of the main web vulnerabilities (choose from the OWASP TOP 10)

Examples of topics covered (depending on participant level and number of days):

- Brute force and fuzzing attacks
- Partitioning and access control
- Exploiting blind SQL injections
- Cross-Site Scripting (XSS) and WAF/CSP bypassing
- Cross-Site Origin Resource Sharing (CORS)
- XML External Entity (XXE)
- Best practices for protecting APIs
  - limited access to resources
  - control mechanism
- File upload form

Web pentest tools presentation

- Burp Pro / OWASP ZAP
- GoBuster / Nmap Scanner Port / SQLMap
- Development of simple operating scripts (Python)

Access to a hands-on lab

- Compromise of a vulnerable application
- In the form of a CTF carried out individually or in teams
- Exploitation of a chain of vulnerabilities to execute system code on the server (RCE)

Getting to grips with the tools

- Getting to grips with the tools
- Lab access
- Burp Free / ZAP: web attack proxies
- Python: a fast, efficient scripting tool

Web services / API security

- API1:2023 - Broken Object Authorization
- API2:2023 - Broken authentication
- API3:2023 - Broken Object Authorization at Property Level
- API4:2023 - Unrestricted Resource Consumption
- API5:2023 - Broken Function Authorization
- API6:2023 - Unrestricted Access to Sensitive Business Streams
- API7:2023 - Server-Side Request Forgery
- API8:2023 - Security misconfiguration
- API9:2023 - Incorrect Inventory Management
- API10:2023 - Unsecured consumption of APIs

Mobile applications

- Secure communications (HTTPS + HSTS)
- General information on Android/iOS application security

Android Security and Pentest training

OWASP Java Training

OWASP training with .NET

Companies concerned

This training course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

Organization

The course alternates theoretical input from the trainer, supported by examples, with brainstorming sessions and group work.

Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

Sanction

A certificate will be issued to each trainee who completes the course.